Exhibit A

U.S. Department of Justice

Tax Division

Emerson Gordon-Marvin
Trial Attorney
Emerson.Gordon-Marvin@usdoj.gov

Mailing Address
150 M Street, N.E.
Washington, D.C. 20002-3388

Phone: (202) 307-0872

October 23, 2025

VIA EMAIL

Jonathan Kravis
Munger, Tolles & Olson LLP
601 Massachusetts Ave. NW, Suite 500E
Washington, DC 20001
jonathan.kravis@mto.com

Re: United States v. Thomas C. Goldstein (8:25-cr-0006-LKG)

Dear Counsel:

At trial, the government anticipates it will call Special Agent Quoc Tuan Nguyen of Internal Revenue Service – Criminal Investigation ("IRS-CI"). Pursuant to Federal Rule of Evidence 16(a)(1)(G), the Government hereby provides notice of its intent to call Agent Nguyen to testify as an expert on select topics, discussed below.

The government reserves the right to offer additional testimony by this expert, or other expert witnesses, and for the experts to amend or adjust their opinions and the bases for those opinions due to information made known to the experts before or during trial.

Publications & Recent Expert Testimony

In the past ten year, Agent Nguyen has authored no publications. In the past four years, Agent Nguyen has not testified an expert in any trial or proceeding.

Experience & Curriculum Vitae

Agent Nguyen's CV is included with this letter. Agent Nguyen is currently an Agent with IRS-CI. He has been an Agent for approximately 14 years. His current duties involve investigation criminal federal tax violations and related financial crimes, including money laundering, identity theft, and financially motivated cybercrimes.

Agent Nguyen started his career with IRS-CI in June 2010 after graduating from Syracuse University with a Bachelor of Science degree in Accounting and Finance, and Master of Science

in Finance. Agent Nguyen was initially hired as an intern and then became a Special Agent in August 2011 after completing the Criminal Investigator Training Program and Agent Investigative Techniques Program at the Federal Law Enforcement Training Center in Glynco, Georgia. The training programs teach financial investigation techniques, with particular focus on investigations involving violations of the Internal Revenue Code (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), and the Money Laundering Control Act of 1986 (Title 18, United States Code, Sections 1956 and 1957).

Agent Nguyen began his career working a wide range of tax and money laundering cases. In the first six years of his career, Agent Nguyen investigated payroll tax cases, tax return preparer cases, embezzlement cases, and an international tax case involving two individuals named in the "Panama Papers" data leak. These cases required Agent Nguyen to analyze bank records and apply his knowledge of tax laws to particular tax returns and propose adjustments, if necessary.

In 2017, Agent became the cybercrime coordinator for the IRS-CI Boston Field Office and was then assigned to the FBI Cybercrime Task Force ("CTF"). As part of the CTF, he primarily investigated financially motivated cybercrimes, including business email comprises, cryptocurrency thefts, financial account takeovers, ransomware, malware and dark web activity. Through his work with the CTF, Agent Nguyen developed specialized skills for cybercrime investigations, including tracing cryptocurrency transactions, geolocating IP addresses, and gathering and interpreting open-source intelligence. In addition, Agent Nguyen gained familiarity with common technical infrastructures and techniques used by cyber criminals, such as using Virtual Private Networks to mask their true location, using offshore hosting services to prevent U.S. law enforcement from obtaining records, and using encryption to secure and conceal communications and data.

In January 2025, Agent Nguyen joined the IRS-CI Western Cybercrimes Unit, which is a specialized group within IRS-CI that focuses on cybercrime investigations. He currently investigates international money brokers laundering narcotics proceeds for transnational drug trafficking organizations, darknet illicit products vendors, and various criminal schemes involving cryptocurrency.

Anticipated Testimony

The Government will offer Agent Nguyen as an expert witness. Agent Nguyen's testimony will assist the jury to understand: (1) how Proton Mail works; (2) why investigators often cannot access the contents of Proton Mail accounts and communications; (3) how Virtual Private Networks ("VPN") work; and (4) how it appears that Defendant used one or more VPNs to access Binance.Com despite its policy banning U.S. users from registering or maintaining an account on their platform.

Defendant's use of Proton Mail, and his decision to email a ledger of 2016 poker transactions to his Proton Mail account (but not his firm manager or his accountants) is described in the Superseding Indictment ("Indictment"), as is his use of a Binance.Com account, which was based abroad. *See* Indictment ¶¶ 33, 83. Both are subjects for which expert testimony is admissible and relevant.

As discussed below, Agent Nguyen's opinions will be based on his experience as a cybercrime investigator; his familiarity with Proton Mail, VPNs, and Binance.Com; evidence introduced at trial (including but not limited to records provided by Binance.Com); and his own, independent analysis of Defendant's Binance.Com access logs and January 22, 2017 email from his [redacted]@goldsteinrussell.com email address to [redacted]@protonmail.com.[1]

Agent Nguyen has been a part of the FBI Cybercrime Task Force since 2017, where he has routinely observed individuals use Proton Mail, and dealt with the investigative challenges posed by Proton Mail's robust encryption capabilities. Agent Nguyen will testify that Proton and its messaging platform, Proton Mail, use both end-to-end and zero-access encryption.

End-to-end ("E2E") encryption is method in which a message is encrypted and only the end users—here, the sender and the receiver—have the encryption key necessary to decrypt the message and view its contents. As a result, if such a message were intercepted or seized by a third party (*i.e.*, someone other than the end users), then that third party would not be able to access or read the contents of the message. E2E encryption is considered one of the most secure methods of communication available to public consumers.

Zero-access encryption is a method used for data storage by some internet service providers, in which the provider (here, Proton) encrypts the user's data and does not, itself, have the encryption key to decrypt the data. The end user, however, still can access and decrypt the data by entering their username and password on Proton Mail online, or using a compatible desktop or mobile application.

In addition, Proton advertises its headquarters and servers are located in Switzerland, which provides a constitutional right to privacy, is outside United States and European Union jurisdiction, and heavily limits what Swiss companies may share with foreign law enforcement. Users often view this as adding an additional level of privacy and security to their communications.

Based on his knowledge about and experience with Proton Mail, as well as his review of the evidence, the Government anticipates that Agent Nguyen will offer the following opinion: the contents of the email account, [redacted]@protonmail.com, would be accessible only to a person that had the login and password (or underlying encryption key) and would not be accessible to Proton, or Swiss or United States authorities without those credentials.

Agent Nguyen also will opine that if a person lost their Proton Mail login and password,[2] and did not have any recovery methods configured, then that person would not be able to access that Proton Mail account and email address, and would have to create a new one if they wanted to continue to use Proton Mail.

[1] This email, with the subject line "file," and its attachment, titled "Amounts.docx," were produced in discovery to Defendant as PROD-USA-0061020 and PROD-USA-0061021.

[2] And (where applicable), if they had configured a desktop or mobile application to access their Proton Mail account, or had downloaded their Proton Mail encryption key—and also had lost access to these options.

Separately, Agent Nguyen will offer his opinion that Defendant used one or more VPNs to create and use a Binance.Com account in 2021. This opinion will be based on his training and experience, access logs provided by Binance.Com, and Agent Nguyen's independent analysis of the Internet Protocol addresses ("IP addresses") of the servers through which Defendant accessed Binance.Com.

Agent Nguyen will explain that all but four of the IP addresses in question resolved to overseas servers often used by VPN service providers, as summarized in the below table.[3] He will also explain that, based on the dates and times at which Defendant used servers in (1) Milan, Italy, (2) Oslo, Norway, and (3) Port of Spain, Trinadad and Tobago, a VPN is the most likely explanation for the pattern of IP addresses recorded by Binance.Com (as opposed to, for example, Defendant traveling to and between, and staying in, those locations).

Summary of Defendant's Binance.Com Access Log

IP Address per Binance.Com	Date First Observed	Date Last Observed	Number of Operations Conducted	Geolocation Per MaxMind	ISP per MaxMind
192.145.127.76	2/6/2021	2/6/2021	3	Port of Spain, Trinidad and Tobago	M247 Europe
84.247.50.62	2/8/2021	2/8/2021	14	Oslo, Norway	M247 Europe
212.102.54.99	2/8/2021	5/5/2021	10	Port of Spain, Trinidad and Tobago	DataCamp
95.174.66.228	2/9/2021	2/9/2021	5	Oslo, Norway	M247 Europe
217.138.197.60	2/11/2021	2/16/2021	18	Milan, Lombardy, Italy	M247 Europe
192.145.127.68	2/23/2021	2/24/2021	9	Port of Spain, Trinidad and Tobago	M247 Europe
138.199.54.232	5/4/2021	5/4/2021	2	Milan, Lombardy, Italy	DataCamp
185.128.27.238	5/12/2021	5/12/2021	3	Port of Spain, Trinidad and Tobago	M247 Europe
217.138.219.153	5/13/2021	5/13/2021	6	Milan, Lombardy, Italy	M247 Europe
212.102.54.104	5/14/2021	5/14/2021	3	Port of Spain, Trinidad and Tobago	DataCamp
138.199.54.238	5/16/2021	5/24/2021	28	Milan, Lombardy, Italy	DataCamp
138.199.54.239	5/19/2021	5/19/2021	3	Milan, Lombardy, Italy	DataCamp
138.199.54.237	5/21/2021	5/21/2021	5	Milan, Lombardy, Italy	DataCamp
104.168.126.146	6/20/2021	6/20/2021	1	Los Angeles, CA, USA	HostPapa

[3] The table, which continues onto the next page, is sorted by the date on which an IP Address was first observed. The four other IP addresses were the last four observed, from June 20, 2021, through January 25, 2022.

IP Address per Binance.Com	Date First Observed	Date Last Observed	Number of Operations Conducted	Geolocation Per MaxMind	ISP per MaxMind
212.193.0.84	7/14/2021	7/14/2021	1	Czechia (CZ), Europe	(*No ISP identified by MaxMind*)
138.59.26.133	7/30/2021	7/30/2021	1	Port of Spain, Trinidad and Tobago	Flow Trinidad
103.110.252.26	1/25/2022	1/25/2022	1	Pune, Maharashtra, India	Goodwill Smartlink Pvt.

In addition, Agent Nguyen may create and aid in the creation of illustrative aids, which the government will seek to use during his testimony pursuant to Rule 107(a). The government may also seek to permit these records to be given to the jury for use in their deliberations, pursuant to Rule 107(b). The government will provide copies of all draft illustrative aids prior to their use at trial.

CONCLUSION

Please do not hesitate to contact us if you have any questions.

Sincerely,

KELLY O. HAYES
United States Attorney

/s/ Emerson Gordon-Marvin
Emerson Gordon-Marvin
Hayter Whitman
Trial Attorneys
Sean Beaty
Senior Litigation Counsel
Department of Justice, Tax Division

Adeyemi Adenrele
Assistant United States Attorney
United States Attorney's Office
District of Maryland

Agent Nguyen's Acknowledgement

I, Quoc Tuan Nguyen, have reviewed and agree with the contents of this disclosure.

Date: October 23, 2025

/s/ *Quoc Tuan Nguyen*
Quoc Tuan Nguyen
IRS-CI Special Agent

QUOC TUAN NGUYEN
IRS-CI SPECIAL AGENT
[redacted] BOSTON, MA [redacted]
[redacted]@CI.IRS.GOV

PROFESSIONAL EXPERIENCE:

Internal Revenue Service, Criminal Investigation · Boston, MA

Special Agent – Western Cybercrimes Unit, January 2025 – Present

- Currently assigned to IRS-CI's Western Cybercrimes Unit, which investigates computer intrusions, money laundering, theft of cryptocurrency, malware, and other cybercrimes
- Currently working an Attorney General Exempt Operation (AEGEO) investigation with DEA targeting international money brokers laundering narcotics proceeds for Mexican and Colombian drug trafficking organizations
- Currently investigating a dark net vendor selling illegal financial products and counterfeit currencies as part of a long-term Organized Crime Drug Enforcement Task Forces (OCDETF) investigation with U.S. Secret Service
- Currently investigating two professional money launderers who are laundering money for foreign criminals by creating offshore shell companies, forming mirror domestic entities, and opening hundreds of domestic and foreign bank accounts
- Currently investigating perpetrators of an investment fraud scam known as "pig butchering" involving cryptocurrency
- Currently investigating an individual who defrauded hundreds of investors by calling himself a seasoned financial advisor and misrepresenting that he would pool their money to trade digital assets, mainly alternative cryptocurrencies

Special Agent – Money Laundering Expert Witness Cadre, January 2021 – Present

- Currently a member of IRS-CI's Money Laundering Expert Witness Cadre, which is a team of Special Agents with extensive field and trial experience in complex money laundering investigations
- Testified in a tax and money laundering trial in the Northern District of Georgia on tracing illicit proceeds using the Last-In, First-Out (LIFO) method through over 120 bank accounts and 56,000 lines of transactions (United States v. Jack Fisher et. al)
    - Testified in criminal trial and forfeiture proceeding

Special Agent – FBI Cybercrimes Task Force, June 2017 – January 2025

- Assigned to the Boston FBI Cybercrimes Task Force, which investigates computer system intrusions, internet fraud, and other financially motivated cybercrimes
- Investigated an international hacker who deployed malware to break into tax preparation firms' computer networks and steal personally identifiable information (PII) to file fraudulent tax returns and applications for various government assistance programs to steal money from the U.S. government
- Investigated two individuals for a scheme to take over victims' social media accounts and steal their cryptocurrency using techniques such as "SIM swapping," computer hacking, and social engineering

- Investigated five individuals for executing a scheme to defraud Coronavirus Aid, Relief and Economic Security (CARES) Act programs by obtaining and using stolen PII to submit fraudulent applications to multiple state unemployment agencies and to submit fraudulent Economic Injury Disaster Loans (EIDL) and Paycheck Protection Program (PPP) loan applications

Special Agent – Boston Field Office, August 2011 – June 2017

- Investigated over 30 money laundering cases ranging from financial fraud to drug trafficking
- Investigated an Australian national living in the U.S. who laundered tens of millions of dollars in proceeds from internet fraud schemes by creating shell companies and opening fraudulent business bank accounts
- Investigated an international $150 million consumer fraud scheme involving the unauthorized placement of charges on consumers' cell phone bills that led to the arrests and convictions of 14 individuals
- Investigated an international investigation that resulted in the first U.S. indictments connected to the Panama Papers leak
- Investigated a financial advisor who embezzled funds from his investors
- Experienced in analysis of financial statements, financial analysis, tracing monetary funds through banking systems, and other forensic accounting
- Prepared treaty requests and obtained evidence from multiple countries, including Canada, Australia, Germany, and Panama
- Participated in search warrants, including as affiant, team leader, evidence custodian, and on-site supervisor
- Prepared case reports and presented findings to the United States Attorney's Office for prosecution
- Testified before grand juries and other court proceedings

EDUCATION:

Syracuse University
Master of Science in Finance, May 2010
Bachelor of Science in Accounting and Finance, May 2009

CERTIFICATIONS:

- Chainalysis Crypto Fundamentals Certification (CCFC)
- Chainalysis Reactor Certification (CRC)
- Chainalysis Investigation Specialist Certification (CISC)

TESTIMONY:

- United States v. Jack Fisher et. al (Northern District of Georgia)
  - Testified in criminal trial and forfeiture proceeding
- United States v. R. David Cohen (District of Massachusetts)
- United States v. Francisco Oscar Grullon (District of Massachusetts)
- United States v. Darcy Wedd (Southern District of New York)

PRESENTATIONS AND SPEAKING ENGAGEMENTS:

- Presenter at IRS-CI's Annual Money Laundering Expert Witness Cadre Training, April 2025
- Delivered blockchain/cyber training to Philippines National Police as part of DoJ's International Criminal Investigative Training Assistance Program (ICITAP), December 2024
- Presenter at the New England National Cyber Crime Conference, April 2023
- Presenter at the New England National Cyber Crime Conference, April 2022
- Presenter at the Manulife/John Hancock Financial Speaker Session, November 2021